To: Examiner Carl Colin (carl.colin@uspto.gov)
From: Benjamin E. Urcia, Reg. No. 33,805
Appl. No. ~~09/763,021~~ 09/763621

Dear Mr. Colin,

The following provides an explanation of why Figs. 2 and 3 show a disguised operation, as claimed, even though only one random number R1 is involved. It is believed that these amendments do not involve "new matter" since they merely explain what is already shown in the drawings, and follow from the original description. In particular, the description uses the term "mapping," which greatly helps facilitate understanding of the invention.

PROPOSED AMENDMENTS TO THE SPECIFICATION

The paragraph bridging pages 4 and 5:

> Figure 3b shows an intermediate step in determining the disguised lookup table of Figure 3c. The lookup table according to Figure 3b was generated from the lookup table according to Figure 3a by XORing each value of the first line of the table from Figure 3a with random number $R_1 = 11$. Thus, XORing the value 00 of the first line and first column of the table from Figure 3a with the number 11 yields the value 11, which is now the element of the first line and first column of the table of Figure 3b. The remaining values of the first line of the table shown in Figure 3b are determined accordingly from the values of the first line of the table shown in Figure 3b are determined accordingly from the values of the first line of the bale shown in Figure 3a and random number $R_1 = 11$. Basically, the XOR function changes 00, 01, 10, and 11 of Fig. 3A to 11, 10, 01, 00. Since h(x) as shown in Fig. 3A maps 00 to 01, 01 to 11, 10 to 10, and 11to 00, the result of disguising the input data would be to map 11 to 00, 10 to 10, 01 to 11, and 00 to 01. However, as shown in Fig. 3B, as a result of the disguised input data x, **the operation is also disguised to become the disguised operation $h_{R1}(x)$**, so that 11 now maps to 01, 10 to 11, 01 to 10 and 00 to 00. The result is that the second line of Fig. 3B is exactly the same as the second line of Fig. 3A, but that the input data is disguised and the operation, in the form of a mapping, is also disguised. ~~The~~ Thus, table shown in Figure 3b could already be used as a disguised lookup table for processing secret data likewise disguised with random number $R_1 = 11$. The result would be the plaintext values to be read in line 2 of this table from Figure 3b. [note to examiner: the highlighting would not be included in the formal amendment]

Page 5, lines 14-16:

> If the table according to Figure 3c, which preserves the mapping or disguised input data and disguised operation of Fig. 3b, is to be disguised further or yield as output values likewise disguised values rather than plaintext values, one applies a further XOR operation with further random number R_2.

Page 2, lines 12-15:

> The security-relevant operation will be represented in the following by function h mapping input data x on output data y, i.e. $y = h(x)$. To prevent secret input data x from being spied out the invention provides, in one example, for a disguised function h_{R1} to be determined, so that the following holds:
>
> $$h(x) = h_{R1} (x \otimes R_1)$$
>
> as shown in Figs.3a-3c, or in a variation of the basic disguising operation, for disguised function h_{R1R2} to be determined, so that the following holds:
>
> $$y \otimes R_2 = h_{R1R2}(x \otimes R_1).$$
>
> as shown in Fig. 3d.

PURPOSE OF AMENDMENTS AND HOW PRIOR ART IS DIFFERENT

The purpose of the amendments is to show that the only randomization needed to disguise the operation is randomization of the input data. Once the randomized input data is generated, it only needs to be mapped to the original result, which is what is shown in Fig. 3b, in order to obtain a disguised function. Thus, the language of claim 1 is correct and supported by the original specification.

Furthermore, even though the randomization operation is only applied to the input data, the result is not the same as the prior art. This is because the prior art randomizes the input data without changing the mapping, as in the following example:

Fig. 3A:

x	00	01	10	11
h(x)	01	11	10	00

disguising x but not changing mapping to disguise operation:

x (disguised, from first row of Fig. 3B)	11	10	01	00
h(x) (using the same mapping as Fig. 3A)	00	10	11	01

To go from the first table to the second table, only the input data is changed. The mapping, and therefore the "operation," does not change. However, in Fig. 3B, the mapping changes as well as the input data, as follows:

disguising x and h (Fig. 3B)

x (disguised)	11	10	01	00
$h_{R1}(x)$ (not same mapping as Fig. 3A)	01	11	10	00

By way of example, in the second table above, 11 still mapped to 00, and 10 still mapped to 10, and so forth, exactly as in the first table. On the other hand, in the third table, the mapping had changed in order to obtain a second row that was the same as the second row of the first table. In other words, in the third table, 11 mapped to 01 rather than 00, 10 mapped to 11 rather than 10, and so forth, and therefore that the *operation* as well as the input data had in fact changed. Thus, it can be seen that Fig. 3b (and Fig. 3c) show both disguised input data and a disguised operation, and that disguising the operation only required a single randomization, as recited in claim 1.

Once it is understood that Fig. 3b shows both the data disguise and the operation disguise, and that h_{R1R2} is not the disguised operation but rather a disguised operation that was further randomized to disguise the *output* data, then the meaning of the following statement in 7-10 on page 5 can be understood: "*The table shown in Figure 3b could already be used as a disguised lookup table for processing secret data likewise disguised with random numbers R_1 = 11.*" This statement in fact supports the claim that a single randomization is used to disguise not only the input data, but also the operation as recited in claim 1–by changing the mapping of the disguised input data to obtain the original output data. In other words, the disguised operation resulted from changing the mapping in the first and second tables above to the mapping in the third table above.